

#2

0p1185

日 本 国 特 許 庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 6月16日

出 願 番 号

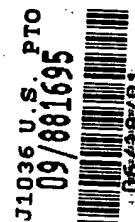
Application Number:

特願2000-182015

出 願 人

Applicant(s):

株式会社 イオノス

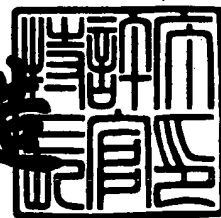


CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月11日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3040178

【書類名】 特許願

【整理番号】 P-7600

【提出日】 平成12年 6月16日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00

【発明の名称】 通信路のスイッチ接続制御装置

【請求項の数】 5

【発明者】

 【住所又は居所】 東京都世田谷区宮坂1丁目36番18号 株式会社 イ
 オノス内

 【氏名】 星野 博一

【特許出願人】

 【住所又は居所】 東京都世田谷区宮坂1丁目36番18号

 【氏名又は名称】 株式会社 イオノス

【代理人】

 【識別番号】 100089244

 【弁理士】

 【氏名又は名称】 遠山 勉

【選任した代理人】

 【識別番号】 100090516

 【弁理士】

 【氏名又は名称】 松倉 秀実

 【連絡先】 03-3669-6571

【手数料の表示】

 【予納台帳番号】 012092

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

| | | |
|-----------|-----|---|
| 【物件名】 | 要約書 | 1 |
| 【プルーフの要否】 | 要 | |

【書類名】 明細書

【発明の名称】 通信路のスイッチ接続制御装置

【特許請求の範囲】

【請求項 1】 通信路に介在され、一方側の通信路との接続と、他方の通信路との接続とを排他的に選択する通信路のスイッチ接続制御装置。

【請求項 2】 データの検証および制御を行う主制御装置と、
第 1 の通信路と接続された第 1 のバッファと、
前記主制御装置に接続され要求またはデータを蓄積する第 2 のバッファと、
前記第 1 のバッファと第 2 のバッファとを短絡・開放する第 1 のスイッチと、
前記主制御装置と第 2 の通信路とを短絡・開放する第 2 のスイッチと、
前記主制御装置からの指示により、前記第 1 または第 2 のいずれか一方のスイッチを排他的に短絡させるための制御信号を出力するスイッチ制御部とからなる通信路のスイッチ接続制御装置。

【請求項 3】 前記第 1 のバッファは、第 1 の通信路からの要求またはデータの正当性を検証する検証手段を備えた請求項 1 記載の通信路のスイッチ接続制御装置。

【請求項 4】 前記主制御装置は、第 2 の通信路からの要求またはデータの正当性を検証する検証手段を備えた請求項 1 記載の通信路のスイッチ接続制御装置。

【請求項 5】 前記に加えて、主制御装置と第 2 のスイッチとの間に要求またはデータを蓄積する第 3 のバッファと、

前記第 2 の通信路と前記第 2 のスイッチとの間に要求またはデータを蓄積する第 4 のバッファとを備えた請求項 2 記載のスイッチ接続制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークにおけるセキュリティに適用して有効な技術に関する

【0002】

【従来の技術】

インターネットの普及は、ビジネス形態を根本から変えるといわれている。

【0003】

データセンターやプロバイダー事業はおろかエンドユーザーまでが、インターネットに常時接続されている昨今、不正なアクセスによる犯罪が盛んになりつつある。いまやセキュリティの導入は政府機構から一個人までその必要性に迫られている。

【0004】

外部ネットワーク（インターネット等）から内部ネットワーク（イントラネット）へのアクセスを防止するためにファイアウォール技術が知られている。

【0005】

このような従来技術のセキュリティは、すべての端末及びシステムが物理上あるいは論理上一本のラインでつながっており、ファイアウォールにより論理的に適正を判断していた。

【0006】

【発明が解決しようとする課題】

従来のネットワークセキュリティ技術では、すべての端末及びシステムが物理上あるいは論理上一本のラインでつながっているため、不正な侵入が可能であるという問題点を抱えている。

【0007】

このためには、外部ネットワークと内部ネットワークとを切り離すことが最も安全である。すなわち、どのような事態（破壊攻撃等）においても一本のラインでつながることがないため、不正な侵入を防御できる。

【0008】

ところが、外部ネットワークから内部ネットワークに対してのアクセス、あるいは内部ネットワークから外部ネットワークへのアクセスが完全に遮断されてしまうと、ネットワーク相互の柔軟な運用が不可能となってしまう。

【0009】

つまり、外部ネットワークと内部ネットワークとを物理的に切り離すことは

アルタイム性や双方向性が損なわれる恐れがある。

【 0 0 1 0 】

本発明は、外部ネットワークからのアクセスに対し、物理的手段によって内部ネットワーク内への直接的な侵入を防ぎつつ、内部ネットワークと外部ネットワークとの柔軟な連携を可能とすることを技術的課題とする。

【 0 0 1 1 】

【課題を解決するための手段】

本発明は、通信路に介在され、一方側の通信路との接続と、他方の通信路との接続とを排他的に選択する通信路のスイッチ接続制御装置である。

【 0 0 1 2 】

すなわち、目的別に分散した端末及びシステムに、シーソー式のスイッチング技術を用い不正侵入を防ぐセキュリティシステムを提供する。

【 0 0 1 3 】

シーソー式のスイッチング技術により、物理的に外部ネットワークと内部ネットワークとを目的に応じたアクセス要求の制御信号によって切り離すため、不正行為から確実にデータを守ることが可能となる。

【 0 0 1 4 】

【発明の実施の形態】

【 0 0 1 5 】

【実施例】

以下、図面に基づいて、本発明の実施の形態を説明する。

【 0 0 1 6 】

図 1 は、本発明の概念を示す機能ブロック図である。

【 0 0 1 7 】

図1に示すように、目的別の端末及びシステムを以下の3つに分類・分散する

【 0 0 1 8 】

同図中、1は、重要なデータやシステムを保有する内部ネットワークであり、コンピュータシステムを通信回線で接続した汎用のネットワークで構成されてい

る。ここで、内部ネットワークとは、上記に示す有線あるいは無線を含めた外線と繋がっていない端末あるいはネットワークを有するシステムを内部ネットワークという。

図中 2 は外部ネットワークである。ここで外部ネットワークとは、インターネット網あるいは公衆網あるいは専用線等の有線あるいは無線を含めた外線と繋がっているネットワークあるいはネットワークを有するシステムあるいは端末あるいはモジュラージャック等のネットワーク構成部品を外部ネットワークという。

3 は、本発明の最も重要な要素となる、内部ネットワークと外部ネットワークとを制御するための制御端末（シーソー式スイッチングセキュリティシステム）である。

【 0 0 1 9 】

制御端末 3 は、さらに、スイッチサーバ 3 1、スイッチ管制部 3 2、バッファ 3 3、バッファ 3 4 およびシーソースイッチングボックス（SSWB） 3 5 とで構成されている。これらの各機能部については後で詳述する。

【 0 0 2 0 】

このシステムにおいて、制御端末 3 は、図 2 に示すように、外部ネットワークからの要求を受信し、内部ネットワークへ送信する機能を有している。また、内部ネットワークのデータを受信し、外部ネットワークへ送信する機能を有している。同図において、シーソースイッチングボックス（SSWB） 5 は、外部ネットワーク 2 からの要求信号を内部ネットワーク 1 に伝えるために、バッファ 3 4 をバッファ 3 3 と接続した状態となっている。

【 0 0 2 1 】

また、制御端末 3 は、図 3 に示すように、内部ネットワークからの要求を受信し、外部ネットワークへ送信する機能を有している。また、外部ネットワークのデータを受信し、内部ネットワークへ送信する機能を有している。同図において、シーソースイッチングボックス（SSWB） 5 は、内部ネットワーク 1 からの要求信号を外部ネットワーク 2 に伝えるために、内部ネットワーク 1 とスイッチサーバ 3 1 とを接続した状態となっている。

【 0 0 2 2 】

制御端末 3 はまた、図 4 に示すように、内部ネットワーク 1 または外部ネットワーク 2 の双方において、要求信号、データ信号を双方向に送受信することも可能である。

【 0 0 2 3 】

このような双方向のモードで使用する場合には、スイッチサーバ 3 1 とシーソースイッチングボックス (S S W B) 3 5 との間にバッファ 3 7 を介装し、さらに内部ネットワーク 1 とシーソースイッチングボックス (S S W B) 3 5 との間にもバッファ 3 6 を介装して、制御端末 3 内が内部ネットワーク 1、外部ネットワーク 2 に対して左右対称構成となるようにしてもよい。この場合、バッファ 3 6 は、内部ネットワークからの要求を外部側スイッチ (S W 2) が閉じるまで、保持する。また、内部ネットワークからの要求に不正なデータがないかを判断し、不正データが検出されるとその要求を破棄するフィルタリングの機能を有する。

【 0 0 2 4 】

バッファ 3 7 は、外部ネットワーク 2 からのデータをスイッチサーバ 3 1 が受け、適正処理されたデータを内部側スイッチ (S W 2) が閉じるまで、保持する機能を有している。

【 0 0 2 5 】

その他の制御端末 3 の動作については、前述の図 2 乃至 3 で説明したものと同様であるので説明は省略する。

【 0 0 2 6 】

なお、制御端末 3 内を左右対称構造としたものは図 4 だけで示したが、このような構造は制御端末 3 をいずれのモードで使用した場合にも適用可能である。

【 0 0 2 7 】

次に、図 5 を用いて、本実施例のオブジェクト分散型ユニット (目的別によって分散されたユニット) における各ユニットの構成、機能及びその動作を説明する。

【 0 0 2 8 】

スイッチサーバ 3 1 は、コンピュータシステムにより構成されており、バスを

中心に中央処理装置（CPU）、メモリ、外部記憶装置、インターフェース（I/O）等で構成されている。外部記憶装置にはプログラムがインストールされており、中央処理装置（CPU）は当該プログラムをメモリにロードして順次実行することによって、スイッチ管制部32に対してシーソーススイッチングボックス（SSWB）35の制御指示信号を出力するようになっている。

【0029】

つまり、スイッチサーバ31は、外部ネットワークからの要求により、内部ネットワークへ必要なデータを要求したり、内部ネットワークから受け取ったデータと外部ネットワークからの要求の整合性を図る等、目的に応じた処理を行う。また、要求やデータ等の信号を元に外部ネットワーク側と内部ネットワーク側のそれぞれのゲート（SW1及びSW2）を排他的に切り替える為の制御信号をスイッチ管制部32に送る。

【0030】

スイッチ管制部32は、中央処理装置（CPU）およびメモリを中心に複数のインターフェース（I/O）で構成されている。すなわち、スイッチサーバ31からの制御指示信号に基づいてシーソーススイッチングボックス（SSWB）35を制御するようになっている。

【0031】

ここで、スイッチ管制部32は、ネットワーク上のデータ信号経路にまったく接触しておらず、スイッチサーバ31、バッファ34、バッファ33、シーソーススイッチングボックス（SSWB）をそれぞれ監視することで、ユニットの状態を管理する役割を有している。

【0032】

そして、バッファ34、バッファ33に対しては、スイッチサーバ31等からの情報を元に各々のモード変更の制御信号を送る。（図13乃至14を参照）

また、スイッチサーバ31に対しては、上記のバッファ34、33のモード状態信号を送る。また、スイッチサーバ31からシーソーススイッチングボックス（SSWB）35へのスイッチ切り替え制御信号を受け、バッファ34、33のモード状態との適正を判断し、シーソーススイッチングボックス（SSWB）に対し

てスイッチ切り替え制御信号を送る機能を有している。

【0033】

バッファ33および34はほぼ同様の構成を有しているが、バッファ34は外部ネットワークに直接接続されている点、バッファ33はシーソーススイッチングボックス（SSWB）35とスイッチサーバ31との間に介装されている点異なる。

【0034】

バッファ34は、外部ネットワークからの要求を外部側スイッチ（SW2）が閉じるまで、保持する。また、外部ネットワークからの要求に不正なデータがないかを判断し、不正データが検出されるとその要求を破棄するフィルタリングの機能を有する。

【0035】

バッファ33は、内部ネットワークからのデータをスイッチサーバ31が受け、適正処理されたデータを外部側スイッチ（SW2）が閉じるまで、保持する機能を有している。

【0036】

シーソーススイッチングボックス（SSWB）35は、フリップフロップ素子（FF）と、スイッチ（SW1、SW2）とで構成されており、フリップフロップ素子（FF）に入力されるスイッチ管制部32からの指示信号Tの値によって、スイッチ1または2のいずれかのスイッチを短絡状態に制御するようになっている。

【0037】

つまり、シーソーススイッチングボックス（SSWB）35は、スイッチ管制部32からの制御信号を受け、フリップフロップ（FF）の動作により、外部ネットワーク2側と内部ネットワーク1側のスイッチ（SW1及びSW2）を排他的に切り替える機能を有している。この点については、図6に真理値表を示してシーソーススイッチングボックス（SSWB）の動作アルゴリズムを説明している。

【0038】

このように、本実施例では、上記に示す各ユニットが、各々明確な役割を持ち

、独立・分散していることで、クラッキング行為や不正侵入から大切なデータを守ることができる。特に、スイッチ管制部32がネットワーク上のデータ信号経路にまったく接触していないため、スイッチサーバ31やバッファ33, 34がクラックされたとしても、それを察知し、シーソースイッチングボックス（SSWB）を制御することができる。

【0039】

この制御方法を利用して、スイッチサーバ31やバッファ33, 34をデュプレックス構造にすれば、クラッキングされたユニットを予備のユニットに自動的に切り替える強化型セキュリティシステムを構築できる。

【0040】

なお、実際の運用に際してスイッチサーバ31が運用モード切替指示（図15のタイミングチャート）を出力するタイミングとしては、以下のようなパターンが考えられる。

【0041】

（1）スイッチサーバへの要求が少ない時間帯に切り替える。

【0042】

スイッチサーバ31へのアクセス状況を基に要求の少ない時間帯を調べ、その時間帯にスイッチサーバへ外部の要求を受け付けられないと、ユーザーには知らせ、その間に内部ネットワークとの通信を行う。

（2）定期的に切り替える。

【0043】

要求のとぎれる時間帯がない場合、あらかじめ指定した時間ごとに接続を外部から内部へ切り替える。切り替える回数を増やすことで1回あたりの内部との通信にかかる時間を減らして、ユーザーの外部ネットワークから要求の遅延を減らすことができる。

（3）ユーザーの要求ごとに切り替える。

【0044】

例えば、内部ネットワークに蓄積している個人情報のうち、ある特定個人の情報を見たい、というアプリケーションの時に、個人情報の問い合わせの都度接続を切り替える。必要最低限の情報のみを外部ネットワーク側へ流すことで、情報を守ることができる。

以上のような（１）乃至（３）の制御は、スイッチサーバ１の記憶装置にインストールされたプログラムに基づいて行われる。

【0045】

次に、図7乃至図10を用いて、本システムの動作を説明する。

【0046】

本システム（SWSEC）内は、物理的に外部ネットワーク２側のスイッチ（SW2）または内部ネットワーク１側のスイッチ（SW1）のいずれか一方しか閉じない（短絡しない構造の）ため、たとえSWSECシステムのスイッチングを制御するスイッチ制御指令または情報受発信サーバ（ここではスイッチサーバ31）がクラッキングされても、内部ネットワークと外部ネットワークが電氣的に導通することはない。

【0047】

また、ネットワーク上のデータ信号経路にまったく接触していない各ユニット（スイッチサーバ31、バッファ34、バッファ33の）制御及び監視機構（ここではスイッチ制御部32）を配置し、スイッチ制御を行うことでクラッキングによる外部からの制御を受付けないようにしている。

【0048】

ここでは、スイッチ35を制御するタイミングを、SWSECシステムが自律的にスイッチングする訳ではなく、スイッチサーバ31が制御指令を出すことにより、外部ネットワーク２から要求の無いときにもスイッチングを行うことができる。スイッチングによって、外部ネットワーク２と切断されている間に要求があった場合は、バッファ34に当該要求が蓄積され、SWSECシステムの接続が外部ネットワーク２側に切り替わった際に当該要求がバッファ34からスイッチサーバ31に伝送される。

【 0 0 4 9 】

スイッチサーバ 3 1 と外部ネットワーク 2 の伝送が途切れなく続く場合は、定期的に内部ネットワーク 1 に接続する時間を設け、守るべきデータを内部ネットワーク 1 に伝送する。伝送中にスイッチサーバ 3 1 から発信すべきデータは、バッファ 3 3 に蓄積される。また、伝送量が多い場合は、守るべき情報以外がはいっている情報サーバ（図示せず）を外部ネットワーク側に設けることで、守らなくてよい情報に対するリクエストを常時受け付けることができる。

【 0 0 5 0 】

次に動作を説明する。

【 0 0 5 1 】

外部ネットワーク 2 側から内部ネットワーク 1 に対して要求があるとその要求信号は、バッファ 3 4 に蓄積される。

【 0 0 5 2 】

ここで、要求が不正なものか正当なものをバッファ 3 4 内の中央処理装置（CPU）が外部記憶装置にインストールされたフィルタプログラムを用いて判断し、不正なものであればその要求を破棄する。

【 0 0 5 3 】

次に、シーソースイッチングボックス（SSWB）のスイッチ（SW2）が切断（開放）されている状態（内部ネットワーク 1 とスイッチサーバ 3 1 とがデータ通信を行っている状態）を示すパケットバッファモードであれば、要求はバッファ 3 4 に蓄積され、シーソースイッチングボックス（SSWB）のスイッチ（SW2）が接続される状態（内部ネットワーク 1 とスイッチサーバ 3 1 がデータ通信を終了している状態）を示すパケットスルーモードになるまで待機する。

【 0 0 5 4 】

内部ネットワーク 1 とスイッチサーバ 3 1 がデータ通信を終了するとスイッチサーバ 3 1 がスイッチ管制部 3 2 にシーソースイッチングボックス（SSWB）3 5 のスイッチの接続をスイッチ（SW1）からスイッチ（SW2）に切り替えるための制御信号を送出する。この制御信号を受け取ったスイッチ管制部 3 2 は、バッファ 3 4 及びバッファ 3 3 の状態がパケットバッファモードになっている

かパケットスルーモードになっているかを監視し、パケットバッファモードになっていれば、パケットスルーモードにするための制御信号を各々バッファ 3 4、3 3 に送出する。そして、パケットバッファモードに変更した通知を示す制御信号を各々バッファ 3 4、3 3 から受け取ると、シーソースイッチングボックス（SSWB）に対してスイッチの接続を SW 1 から SW 2 に切り替えるための制御信号を送出する。また、パケットスルーモードになっていれば、シーソースイッチングボックス（SSWB）3 5 にスイッチの接続を SW 1 から SW 2 に切り替えるための制御信号を送出する。

【 0 0 5 5 】

前記要求は、シーソースイッチングボックス（SSWB）のスイッチ（SW 2）及びバッファ 3 3 を経由して、スイッチサーバ 3 1（スイッチング制御及び情報受発信サーバ）に入力される。

【 0 0 5 6 】

スイッチサーバ 3 1 では、前記で入力された要求の適正及び目的を、中央処理装置（CPU）がフィルタプログラムを用いて判断し、不正なものであればその要求を破棄する。

【 0 0 5 7 】

要求が適正である場合には、シーソースイッチングボックス（SSWB）3 5 のスイッチの接続を SW 2 から SW 1 に切り替えるための制御信号をスイッチ管制部 3 2 に送る。

【 0 0 5 8 】

この制御信号を受信したスイッチ管制部 3 2 は、バッファ 3 4 及びバッファ 3 3 の状態をパケットバッファモードにするための制御信号を各々バッファ 3 4、3 3 に送出する。そして、パケットバッファモードに変更した通知を示す制御信号を各々バッファ 3 4、3 3 から受け取ると、シーソースイッチングボックス（SSWB）3 5 に対してスイッチの接続を SW 2 から SW 1 に切り替えるための制御信号を送出する。

【 0 0 5 9 】

次に、スイッチ管制部 3 2 から送られてきた制御信号をシーソースイッチング

ボックス（SSWB）35が受け取るとフリップフロップ（FF）の動作により、スイッチの接続をSW2からSW1に切り替える（図8参照）。

【0060】

スイッチサーバ31は、内部ネットワーク1側に目的に合った要求を送出する。

【0061】

次に、内部ネットワーク1は、図9に示すように、スイッチサーバ31より送られてきた要求により、データを送出する。

【0062】

当該データは、シーソーススイッチングボックス（SSWB）の短絡状態のスイッチ（SW1）を経由して、スイッチサーバ31に送られる。

【0063】

スイッチサーバ31は、そのデータを目的に合った適正な形式に形成する。この成形は外部記憶装置にインストールされたプログラムに基づいて中央処理装置（CPU）が行う。

【0064】

次に、スイッチサーバ31は、シーソーススイッチングボックス（SSWB）のスイッチの接続をSW1からSW2に切り替えるための制御信号をスイッチ制御部32に送ると同時に、パケットバッファモードになっているバッファ33に前記で成形されたデータを送出する。

【0065】

スイッチサーバ31からの制御信号を受け取ったスイッチ制御部32は、シーソーススイッチングボックス（SSWB）35にスイッチの接続をSW1からSW2に切り替えるための制御信号を送出する。続いて、バッファ33の状態をパケットスルーモードにするための制御信号をバッファ33に送出し、パケットスルーモードに変更した通知を示す制御信号をバッファ33から受け取る。

【0066】

次に、図10に示すように、データがバッファ33からシーソーススイッチングボックス（SSWB）35のスイッチ（SW2）を経由して、パケットバッファ

モードになっているバッファ 3 4 に入力される。

【 0 0 6 7 】

バッファ 3 3 は、データを送信し終わるとその通知信号（バッファエンプティ信号）をスイッチ管制部 3 2 に送出する。バッファエンプティ信号を受け取ったスイッチ管制部 3 2 は、パケットバッファモードになっているバッファ 3 4 に対してパケットスルーモードにするための制御信号を送出する。

【 0 0 6 8 】

この制御信号を受け取ったバッファ 3 4 は、自身の状態をパケットスルーモードにし、パケットスルーモードに変更した通知を示す制御信号をスイッチ管制部 3 2 に返信する。

【 0 0 6 9 】

このようにしてデータが外部ネットワーク 2 に伝送される。

次に、本実施例の適用例を図 1 1 を用いて説明する。

【 0 0 7 0 】

同図では、たとえば、インターネットショッピングにおける個人 ID とユーザー属性の認証行為をプロバイダに置いているウェブサーバ 1 1 0 2 から企業内に設置されたデータサーバ（内部ネットワーク 1）へ要求された場合を想定している。

【 0 0 7 1 】

外部ネットワーク 2 は、インターネット 2 1 に接続されており、当該インターネット 2 1 は、ルータ 1 1 0 1 を介してプロバイダのウェブサーバ 1 1 0 2 に接続されている。このウェブサーバ 1 1 0 2 は、ルータ 1 1 0 3 を介してインターネット 2 2 に接続され、当該インターネット 2 2 にはユーザ端末 1 1 0 4 が接続されている。

【 0 0 7 2 】

同図の場合、外部ネットワーク 2 からの認証要求に基づいて内部ネットワーク 1 から認証結果をデータとして出力する動作を行うが、この動作は前述の図 7 乃至図 1 0 の説明で実現される。

【 0 0 7 3 】

図 1 2 は、個人の家庭内に設置された端末装置 2 1 が内部ネットワークに該当し、外部ネットワークであるプロバイダのウェブサーバ 1 2 0 3 に対して楽曲データのダウンロード要求を送信し、これに対してウェブサーバ 1 2 0 3 から楽曲データを受信する場合の構成である。

【 0 0 7 4 】

同図において、ルータやモジュラージャック 2 1 を介して、インターネット 1 2 0 1 に接続されており、当該インターネット 1 2 0 1 は、ルータ 1 2 0 2 を経由してプロバイダのウェブサーバ 1 2 0 3 に接続されている。ウェブサーバ 1 2 0 3 には音楽配信用の楽曲データが蓄積されている。

【 0 0 7 5 】

このような音楽配信サービスにおいて、個人の端末装置 1 1 からウェブサーバ 1 2 0 3 に対して楽曲データの送信を要求する。当該要求がウェブサーバ 1 2 0 3 で受信されこれが図示しない方法で認証されると、ウェブサーバ 1 2 0 3 から楽曲データがインターネット 1 2 0 1 を介してルータ及びモジュラージャック 2 1 を経由して制御端末 3 に受信される。このときの要求の発信からデータの受信の手順については、前述の図 7 乃至図 1 0 の説明で同様に実現することができる。ただし、前述の図 7 乃至図 1 0 の説明において、「要求」を「データ」、「データ」を「要求」と読み替える必要がある。

【 0 0 7 6 】

また、以上の適用例以外にも、企業内 LAN やプロバイダー内、データセンター事業、個人用 PC 端末などにおいても本システムを介在させることが可能である。すなわち、本発明は、前述の実施例およびその適用例に限定されるものではなく、ネットワーク上の如何なる部分にも介在させることができ、ネットワーク毎の内部セキュリティを維持することが可能である。

【 0 0 7 7 】

【発明の効果】

本発明によれば、外部ネットワークと内部ネットワークとを目的に応じたアクセス要求の制御信号によって切り離すため、リアルタイム性や双方向性が損なわ

れることなくデータのやり取りが可能となる。

【図面の簡単な説明】

【図 1】 本発明の原理構成を示すブロック図（1）

【図 2】 本発明の原理構成を示すブロック図（2）

【図 3】 本発明の原理構成を示すブロック図（3）

【図 4】 本発明の原理構成を示すブロック図（4）

【図 5】 実施例の詳細な機能ブロック図

【図 6】 実施例のシーソーススイッチングボックス（SSWB）の構成および

真理値表

【図 7】 実施例の接続制御装置動作説明図（1）

【図 8】 実施例の接続制御装置動作説明図（2）

【図 9】 実施例の接続制御装置動作説明図（3）

【図 10】 実施例の接続制御装置動作説明図（4）

【図 11】 実施例の適用例を示すシステム図（1）

【図 12】 実施例の適用例を示すシステム図（2）

【図 13】 実施例において外部通信モードから内部通信モードへの移行手順を示すフロー図

【図 14】 実施例において内部通信モードから外部通信モードへの移行手順を示すフロー図

【図 15】 実施例の接続制御装置のタイミングチャート

【符号の説明】

1 内部ネットワーク

2 外部ネットワーク

2 1 インターネット

2 2 インターネット

3 制御端末（制御装置）

3 1 スイッチサーバ

3 2 スイッチ管制部

3 3 バッファ（第 2 バッファ）

3 4 バッファ (第 1 バッファ)

3 5 シーソースイッチングボックス (S S W B)

1 1 0 1 ルータ

1 1 2 0 ウェブサーバ

1 1 0 3 ルータ

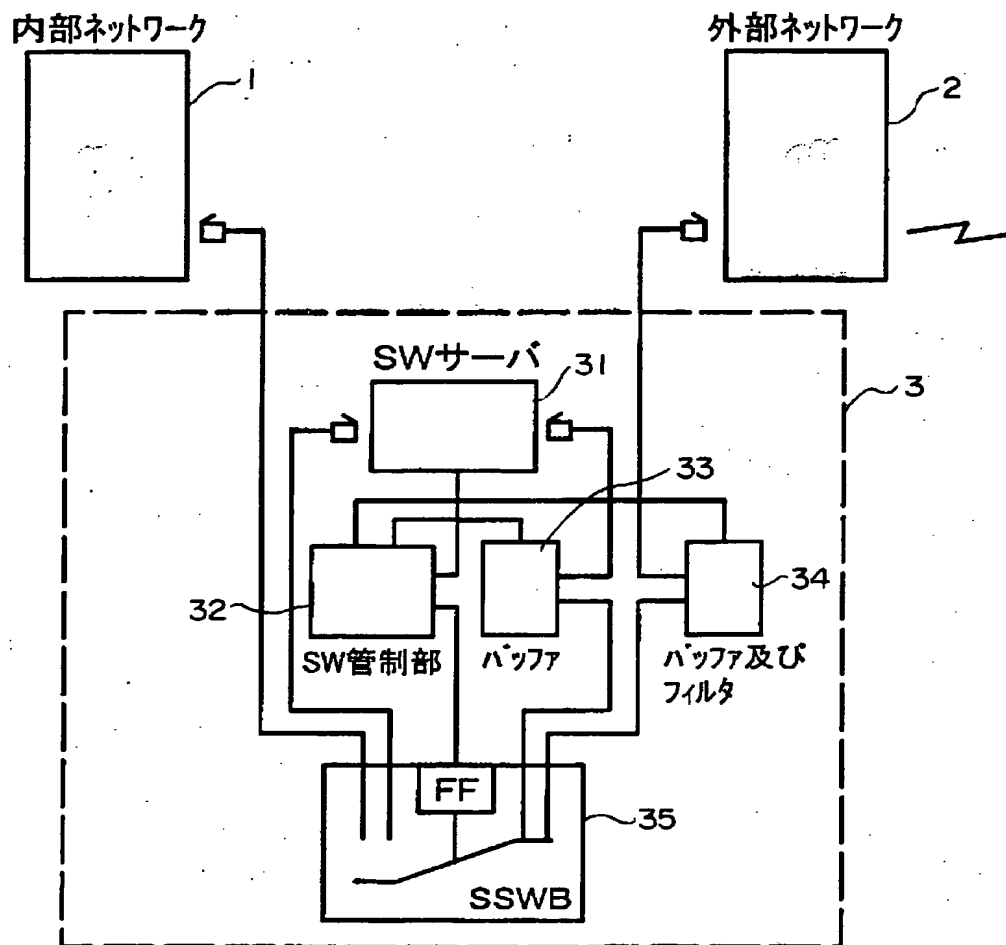
1 1 0 4 ユーザ端末

1 2 0 1 インターネット

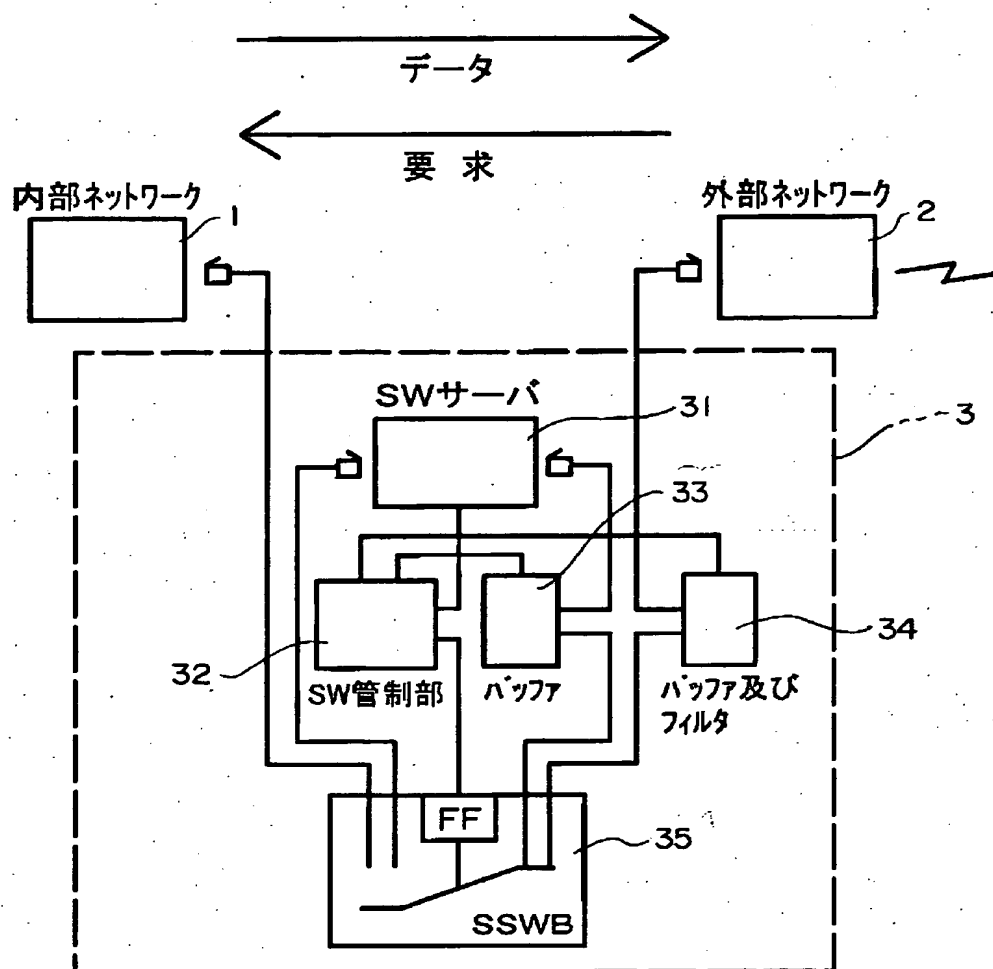
1 2 0 3 ウェブサーバ

【書類名】 図面

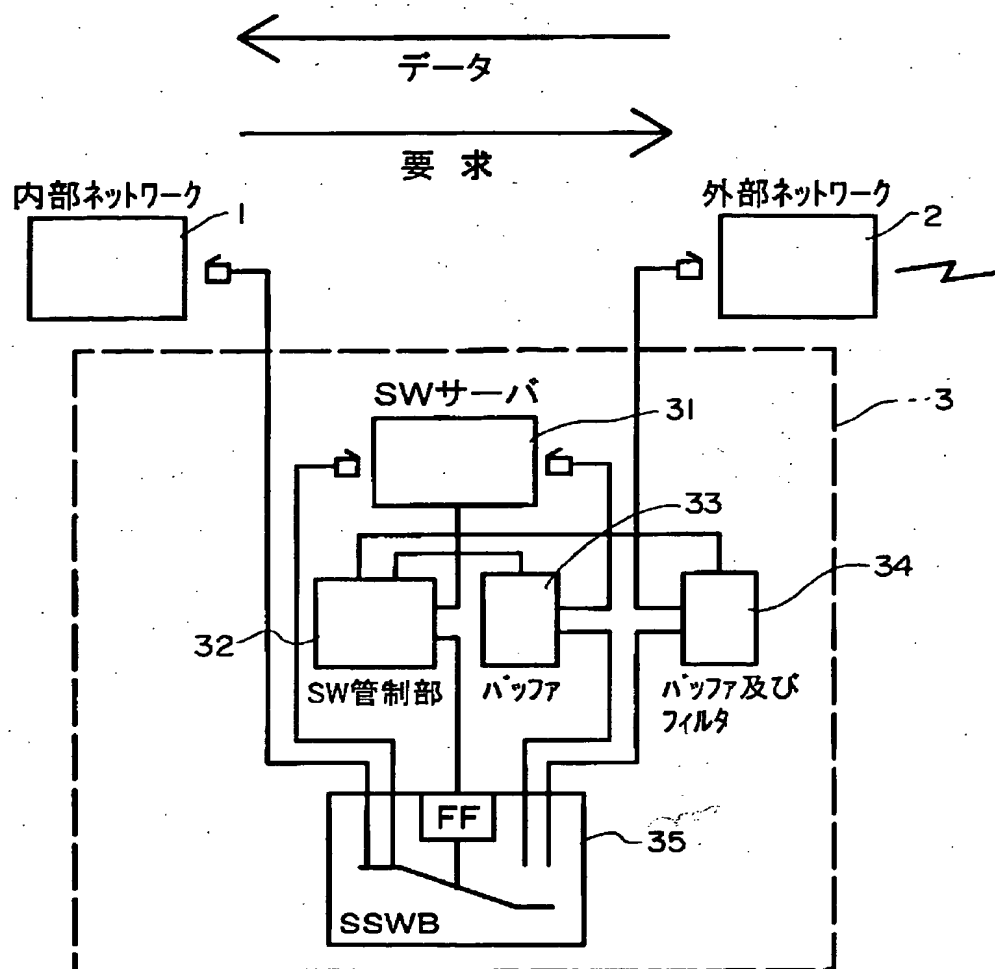
【図1】



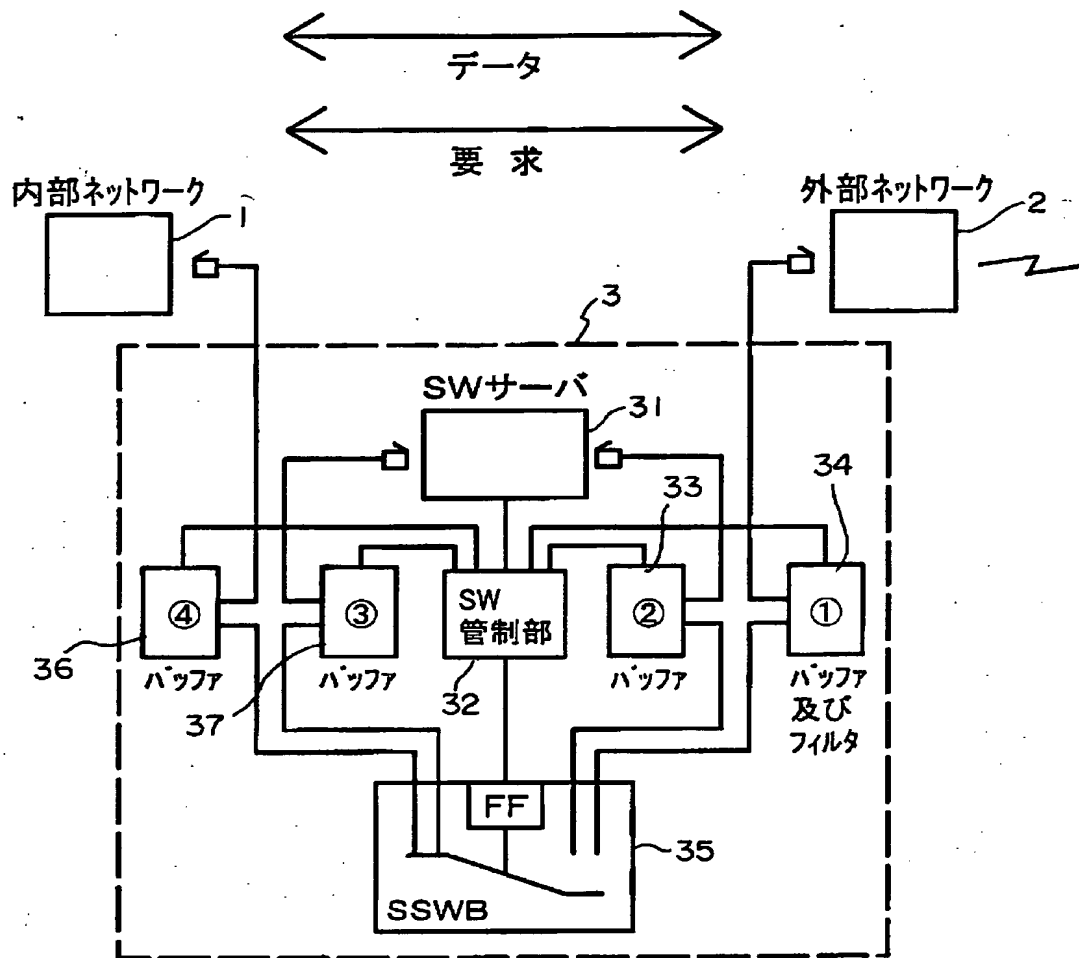
【図2】



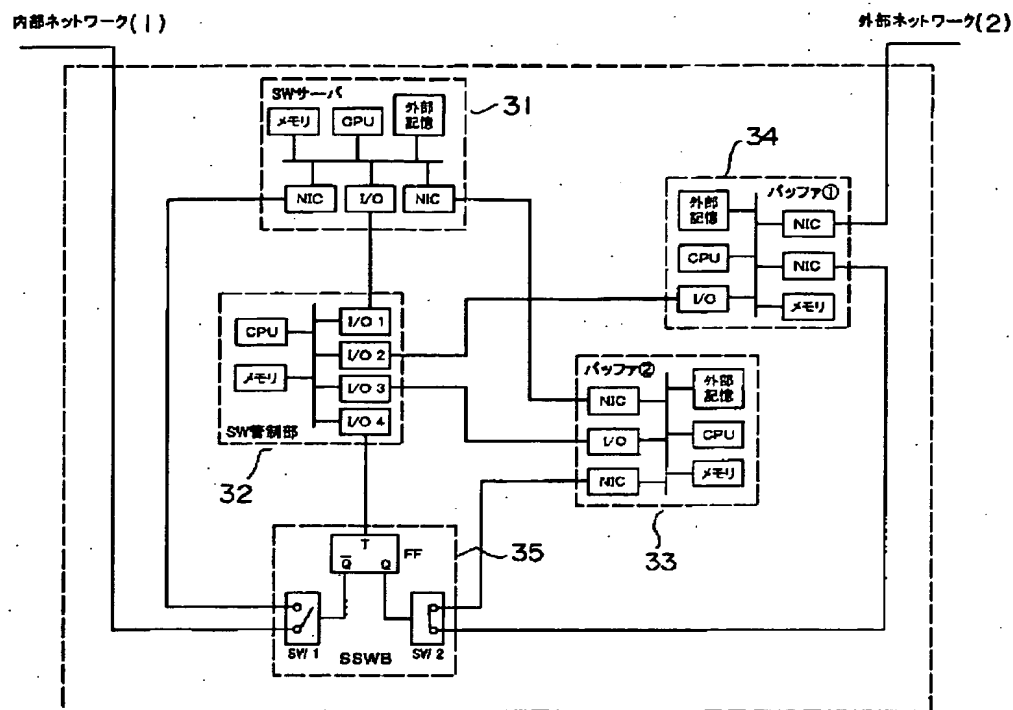
【図3】



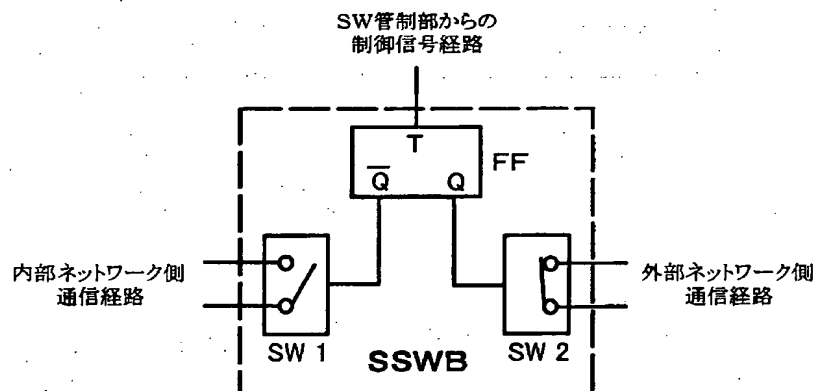
【図4】



【図 5】



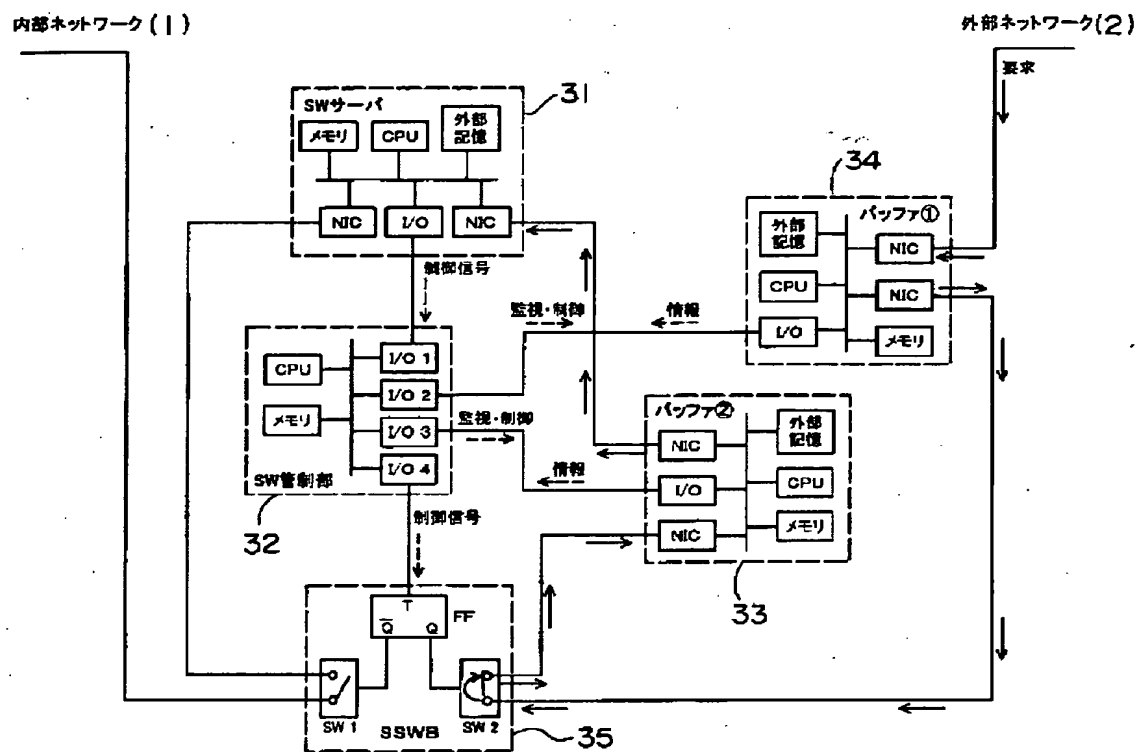
【図 6】



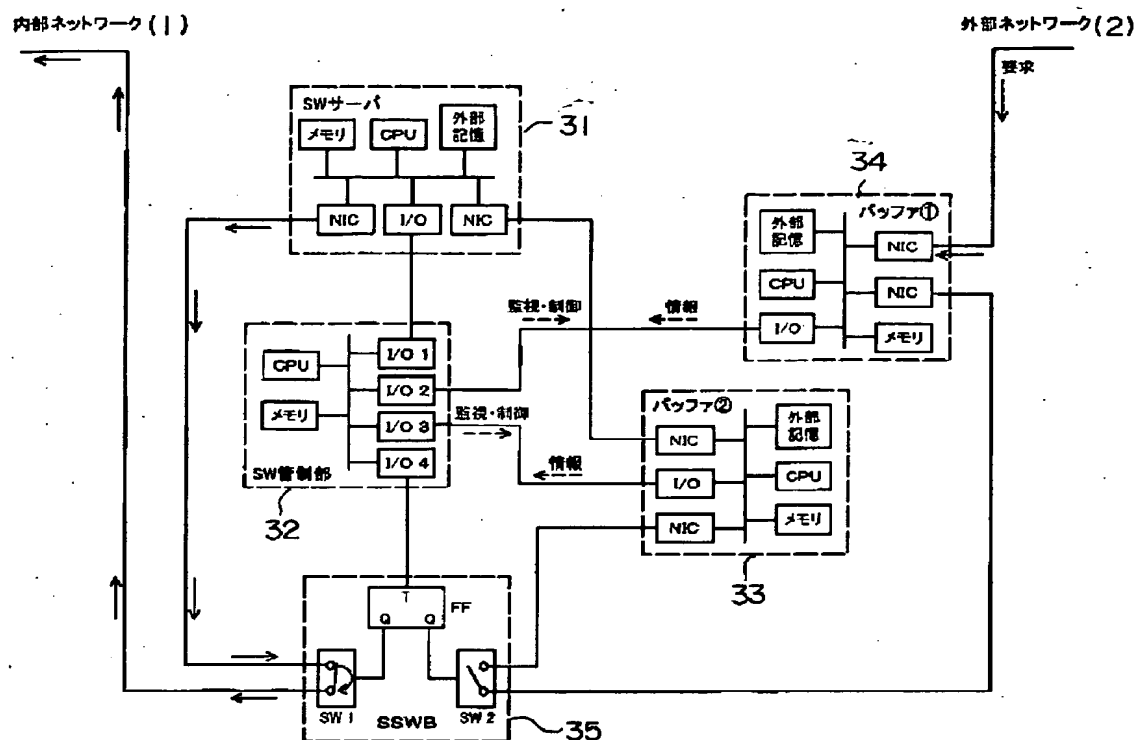
< SW1とSW2を制御するカットフリップフロップの真理値表 >

| T | Q | \bar{Q} |
|---|-------|-----------|
| 0 | 変化しない | |
| 1 | 反転する | |

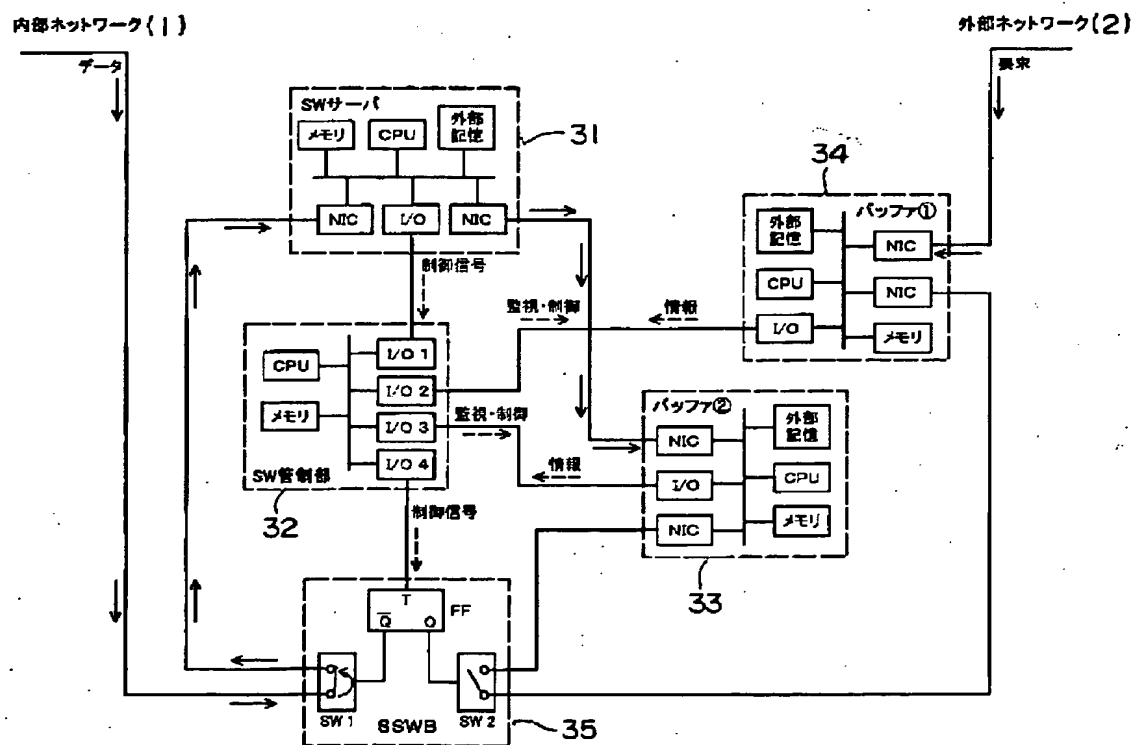
【図 7】



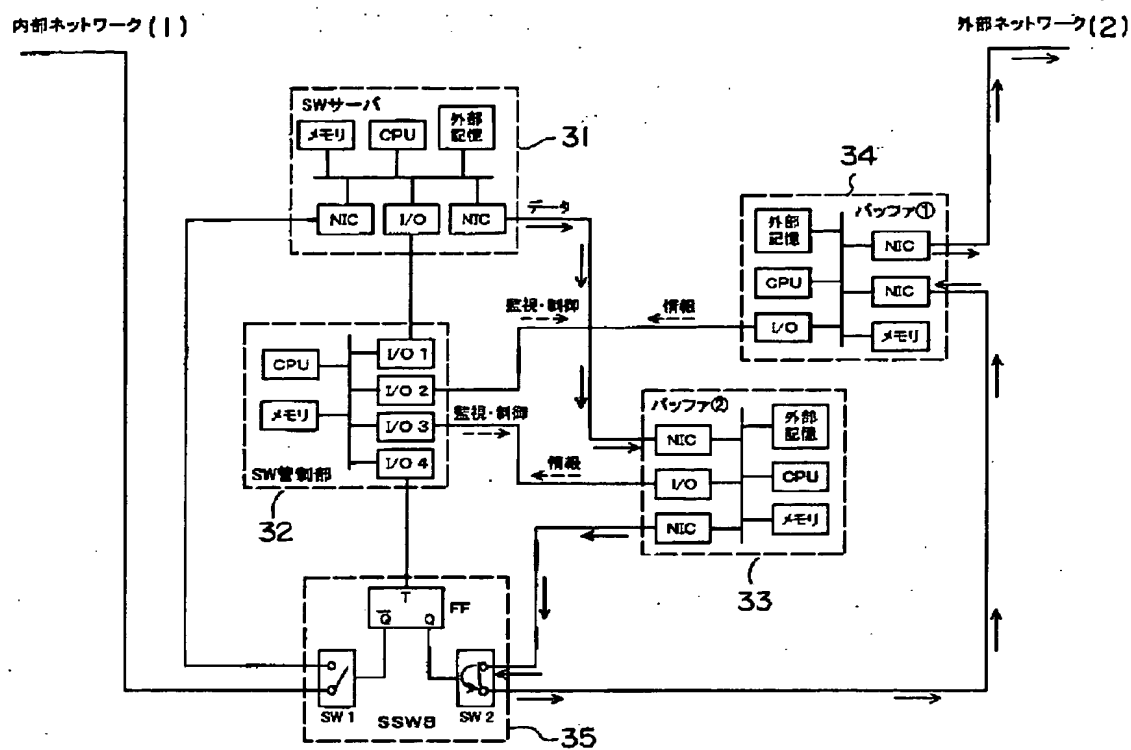
【図 8】



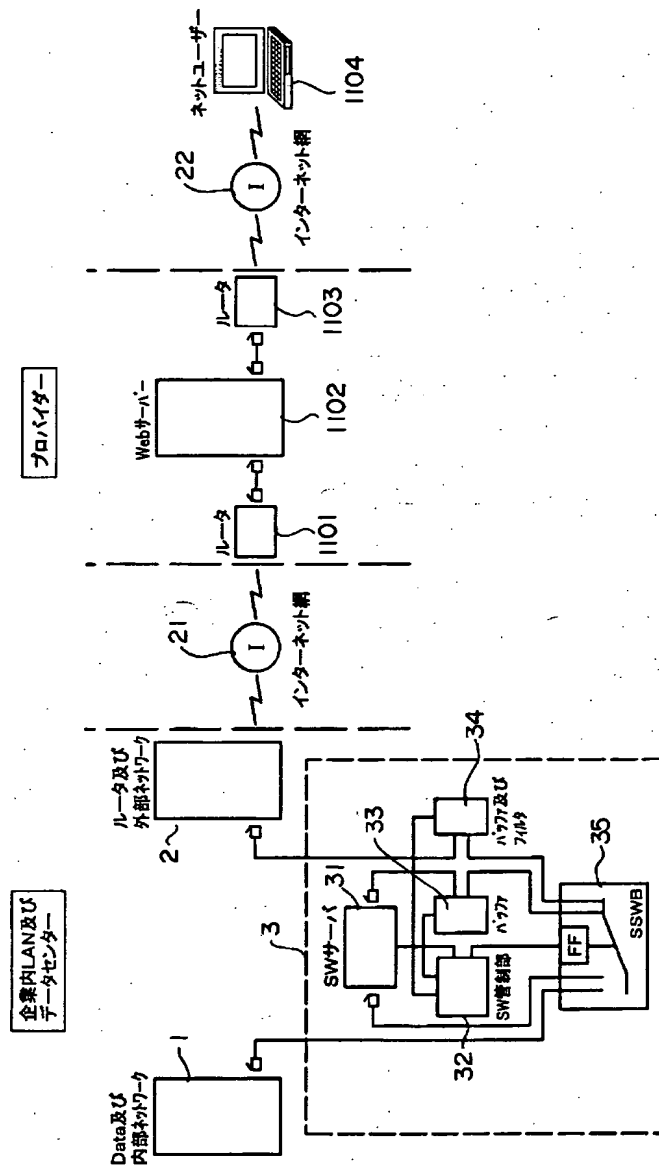
【図 9】



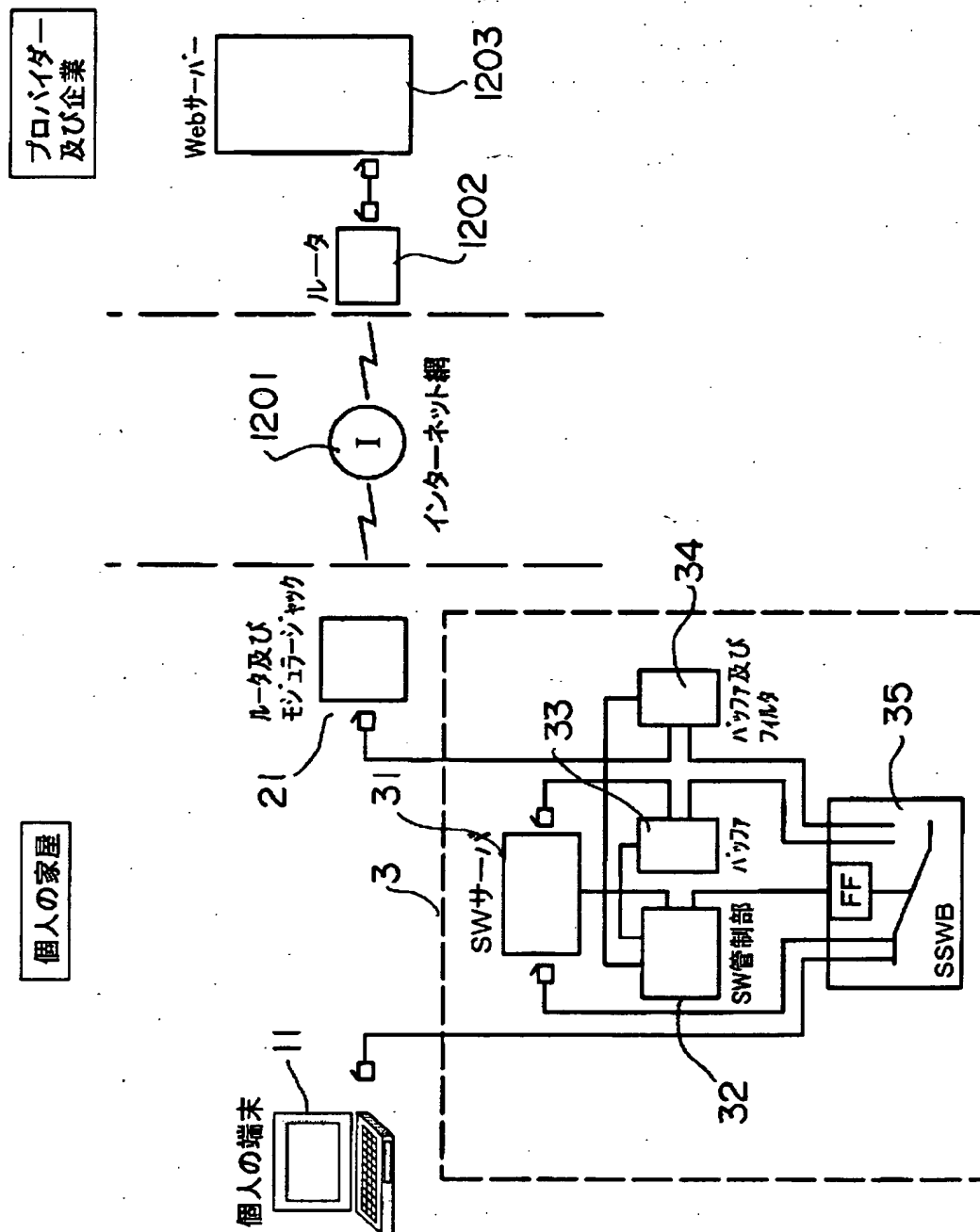
【図10】



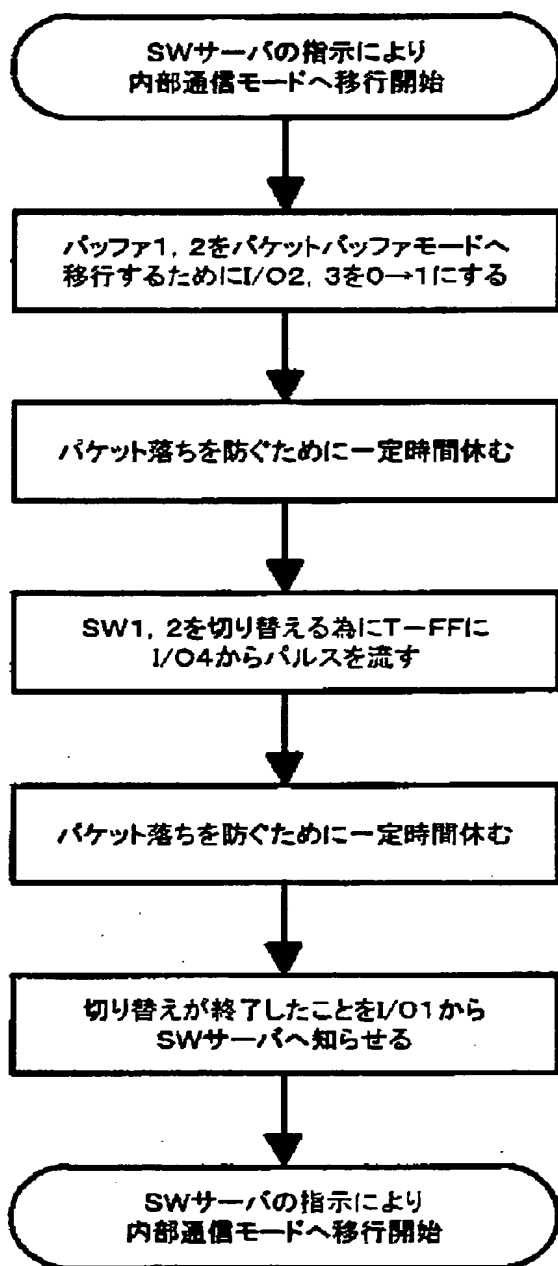
【図11】



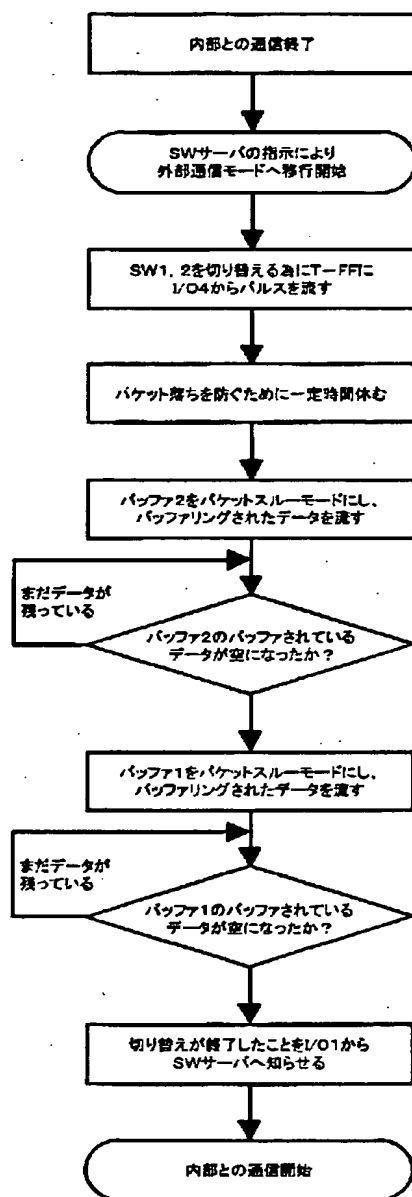
【図 12】



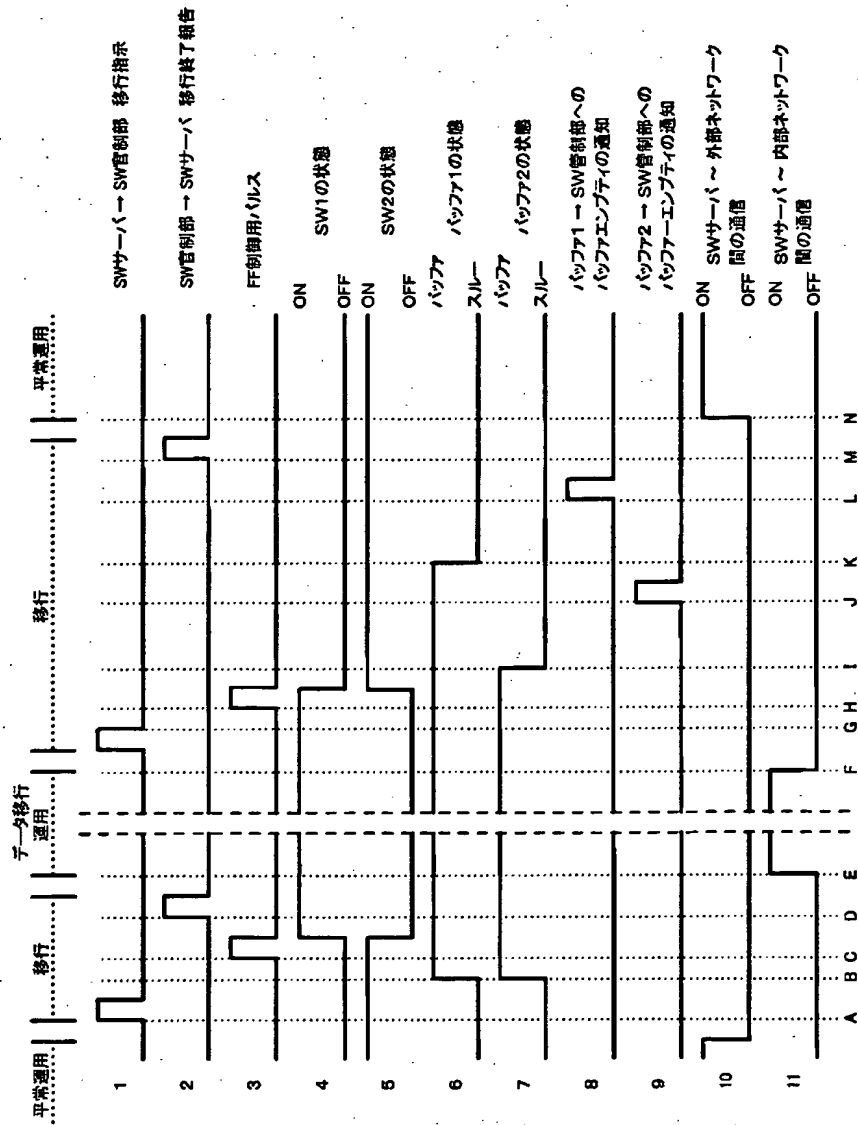
【図13】



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 外部ネットワークからのアクセスに対し、物理的手段によって内部ネットワーク内への直接的な侵入を防ぎつつ、内部ネットワークと外部ネットワークとの柔軟な連携を可能とする。

【解決手段】 通信路に介在させ、一方側の通信路との接続と、他方の通信路との接続とを排他的に選択する通信路のスイッチ接続制御装置とすることにより、目的別に分散した端末及びシステムに、シーソー式のスイッチング技術を用い不正侵入を防ぐセキュリティシステムを提供する。このようにシーソー式のスイッチング技術により、物理的に外部ネットワークと内部ネットワークとを目的に応じたアクセス要求の制御信号によって切り離すため、不正行為から確実にデータを守ることが可能となる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [500283088]

1. 変更年月日 2000年 6月16日
[変更理由] 新規登録
住 所 東京都世田谷区宮坂1丁目36番18号
氏 名 株式会社 イオノス